Polismyndigheten
Box 12256
102 26 Stockholm

Tillsyn enligt brottsdatalagen (2018:1177) – Polismyndighetens rutiner för hantering av personuppgiftsincidenter

Innehållsförteckning

Datainspektionens beslut

Datainspektionen meddelar följande rekommendationer med stöd av 5 kap. 6 § brottsdatalagen (2018:1177):

1. Polismyndigheten bör regelbundet utvärdera effektiviteten hos de vidtagna säkerhetsåtgärderna för att upptäcka personuppgiftsincidenter och vid behov revidera dessa för att upprätthålla tillräckligt skydd av personuppgifter.

2. Polismyndigheten bör regelbundet kontrollera att rutinerna för hantering av personuppgiftsincidenter följs.

3. Polismyndigheten bör, i myndighetens rutiner för dokumentation av personuppgiftincidenter, komplettera med vilka effekter som följer med en incident och vilka korrigerande åtgärder som vidtagits med anledning av den. Därutöver bör Polismyndigheten regelbundet kontrollera att rutinerna för dokumentation av personuppgiftsincidenter följs.

4. Polismyndigheten bör ge sina anställda löpande information och återkommande utbildning i hanteringen av personuppgiftsincidenter och om rapporteringsskyldigheten.

Datainspektionen avslutar ärendet.

Redogörelse för tillsynsärendet

Skyldigheten för den personuppgiftsansvarige – dvs. privata och offentliga aktörer – att anmäla vissa personuppgiftsincidenter till Datainspektionen infördes den 25 maj 2018 genom dataskyddsförordningen[1] (GDPR). Motsvarande anmälningsskyldighet infördes den 1 augusti 2018 i brottsdatalagen (BDL) för s.k. behöriga myndigheter.[2] Skyldigheten att anmäla personuppgiftsincidenter (nedan kallad incident) syftar till att stärka integritetsskyddet genom att Datainspektionen får information om händelsen och kan välja att vidta åtgärder när inspektionen bedömer att det behövs för att den personuppgiftsansvarige ska hantera incidenten på ett tillfredställande sätt och vidta åtgärder för att förhindra att något liknande inträffar igen.

En personuppgiftsincident är enligt 1 kap. 6 § BDL en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring, eller obehörigt röjande av eller obehörig åtkomst till personuppgifter. I förarbetena till lagen anges att det som regel är fråga om en oplanerad händelse som påverkar säkerheten för personuppgifterna på ett negativt sätt och som medför allvarliga konsekvenser för skyddet av uppgifterna.[3] En personuppgiftsincident kan till exempel vara att personuppgifter har skickats till fel mottagare, att tillgången till personuppgifterna har förlorats, att datautrustning som lagrar personuppgifter har tappats bort eller stulits, att någon inom eller utanför organisationen tar del av information som den saknar behörighet till.

En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan medföra risker för den registrerades rättigheter eller friheter. En incident kan leda till fysisk, materiell eller immateriell skada genom exempelvis

---

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

[2] En behörig myndighet är enligt i 1 kap. 6 § BDL en myndighet som behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

[3] Prop.2017/18:232 s. 438

diskriminering, identitetsstöld, identitetsbedrägeri, skadat anseende, finansiell förlust samt brott mot sekretess eller tystnadsplikt.

Det kan finnas många orsaker till att en personuppgiftincident uppstår. Av Datainspektionens rapportserie *Anmälda personuppgiftsincidenter* under perioden maj 2018 - december 2019 framgår att de vanligaste orsakerna bakom de anmälda incidenterna var bl.a. den mänskliga faktorn, tekniska fel, antagonistiska angrepp samt brister i organisatoriska rutiner eller processer.[4]

Datainspektionen har inlett detta tillsynsärende mot Polismyndigheten i syfte att kontrollera om myndigheten har rutiner på plats för att upptäcka personuppgiftsincidenter och om myndigheten har och har haft rutiner för att hantera personuppgiftsincidenter enligt brottsdatalagen. I granskningen ingår även att kontrollera om Polismyndigheten har rutiner för dokumentation av incidenter som svarar mot kraven i brottsdataförordningen (BDF) samt om myndigheten har genomfört informations- och utbildningsinsatser kring personuppgiftsincidenter.

Tillsynen inleddes med en skrivelse till Polismyndigheten den 19 juni 2019 och följdes upp med begäran om komplettering den 28 januari 2020 samt den 12 maj 2020. Myndighetens svar på tillsynsskrivelsen kom in den 19 september 2019 och kompletteringarna inkom den 6 mars 2020 respektive den 28 maj 2020.

Tillämpliga bestämmelser

Den personuppgiftsansvarige ska enligt 3 kap. 2 § BDL, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Det innebär att behöriga myndigheter, med hjälp av dessa åtgärder, inte bara ska säkerställa att dataskyddsregelverket följs utan också ska kunna visa att så är fallet. Vilka

[4] Se Datainspektionens rapportserie om Anmälda personuppgiftsincidenter 2018 (Datainspektionens rapport 2019:1) s 7 f; Anmälda personuppgiftsincidenter januari-september 2019 (Datainspektionens rapport 2019:3) s.10 f. och Anmälda personuppgiftsincidenter 2019 (Datainspektionens rapport 2020:2) s. 12 f.

tekniska och organisatoriska åtgärder som krävs för att skydda personuppgifterna regleras i 3 kap. 8 § BDL.
I förarbetena till lagen anges att organisatoriska åtgärder som avses i 2 § är bl.a. att ha interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Åtgärder som vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av IT-system, behandlingar och vidtagna åtgärder och teknisk spårbarhet genom loggning och logguppföljning. Vilka åtgärder som ska vidtas får avgöras efter en bedömning i varje enskilt fall.[5] Åtgärderna ska ses över och uppdateras vid behov. De åtgärder som den personuppgiftsansvarige ska vidta enligt denna bestämmelse ska enligt 3 kap. 1 § BDF vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

Av 3 kap. 8 § BDL framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. I förarbetena till brottsdatalagen anges att säkerheten ska omfatta åtkomstskydd för utrustning, kontroll av datamedier, lagringskontroll, användarkontroll, åtkomstkontroll, kommunikationskontroll, indatakontroll, transportkontroll, återställande, driftsäkerhet och dataintegritet. Denna uppräkning är dock inte uttömmande. Som exempel på organisatoriska säkerhetsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner. Rutiner för anmälan och uppföljning av personuppgiftsincidenter utgör också sådana åtgärder.[6]

Vilka omständigheter som bör beaktas för att uppnå en lämplig skyddsnivå är reglerat i 3 kap. 11 § BDF. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheterna, kostnaderna för åtgärderna, behandlingens art, omfattning, sammanhang och ändamål, samt de särskilda riskerna med behandlingen. Särskild hänsyn bör tas till i vilken

[5] Prop. 2017/18:232 s. 453
[6] Prop. 2017/18:232 s. 457

utsträckning känsliga personuppgifter behandlas och hur integritetskänsliga övriga personuppgifter som behandlas är.[7] Överträdelse av bestämmelser i 3 kap. 2 och 8 §§ BDL kan leda till sanktionsavgifter enligt 6 kap. 1 § 2 BDL. Den personuppgiftsansvarige ska enligt 3 kap. 14 § BDF dokumentera alla personuppgiftsincidenter. Dokumentationen ska redovisa omständigheterna kring incidenten, dess effekter och de åtgärder som vidtagits med anledning av den. Den personuppgiftsansvarige ska dokumentera alla inträffade incidenter oavsett om den måste anmälas till Datainspektionen eller inte.[8] Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av den aktuella bestämmelsen. Underlåtenhet att dokumentera personuppgiftsincidenter kan föranleda sanktionsavgifter enligt 6 kap. 1 § BDL.

En personuppgiftsincident ska också, enligt 3 kap. 9 § BDL, anmälas till Datainspektionen senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om incidenten. En anmälan behöver inte göras om det är osannolikt att incidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet. Av 3 kap. 10 § BDL framgår att den personuppgiftsansvarige i vissa fall ska informera den registrerade som berörs av incidenten. Underlåtenhet att anmäla en personuppgiftsincident till Datainspektionen kan leda till administrativa sanktionsavgifter enligt 6 kap. 1 § BDL.[9]

Motivering av beslutet

Datainspektionens granskning

Datainspektionen har i detta tillsynsärende att ta ställning till om Polismyndigheten har dokumenterade rutiner för att upptäcka personuppgiftsincidenter enligt brottsdatalagen och om myndigheten har och har haft rutiner för att hantera incidenter sedan BDL trädde ikraft. Granskningen omfattar även frågan om efterlevnaden av kravet på dokumentation av incidenter i 3 kap. 14 § BDF. Därutöver ska Datainspektionen ta ställning till om Polismyndigheten har genomfört

[7] Prop. 2017/18:232 s. 189 f.
[8] Prop. 2017/18:232 s. 198
[9] Ansvaret för överträdelser är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut, se prop. 2017/18:232 s. 481.

informations- och utbildningsinsatser för sina anställda med fokus på hantering av personuppgiftsincidenter enligt BDL.

Granskningen omfattar inte innehållet i rutinerna eller utbildningsinsatserna utan är fokuserad på att kontrollera att den granskande myndigheten har rutiner på plats och att den har genomfört utbildningsinsatser för medarbetarna avseende personuppgiftsincidenter. Granskningen omfattar dock om myndighetens rutiner innehåller anvisningar att dokumentera de uppgifter som krävs enligt brottsdataförordningen.

Rutiner för att upptäcka personuppgiftsincidenter

De personuppgifter som behöriga myndigheter hanterar inom ramen för sin brottsbekämpande och brottsutredande verksamhet är i stor utsträckning av känslig och integritetskänslig natur. Verksamhetens karaktär ställer höga krav på de brottsbekämpande myndigheternas förmåga att skydda de registrerades uppgifter genom nödvändiga skyddsåtgärder för att bl.a. förhindra att en incident uppstår.

Skyldigheten att rapportera personuppgiftsincidenter enligt 3 kap. 9 § BDL ska tolkas i ljuset av de generella kraven att vidta lämpliga tekniska och organisatoriska åtgärder, för att säkerställa lämplig säkerhet för personuppgifter, som föreskrivs i 3 kap. 2 och 8 §§. En förmåga att snabbt upptäcka och rapportera en incident är en nyckelfaktor. För att de brottsbekämpande myndigheterna ska kunna leva upp till rapporteringskravet måste de ha interna rutiner och tekniska möjligheter för att upptäcka en incident.

Utifrån verksamhetens behov och med stöd av risk- och sårbarhetsanalyser kan behöriga myndigheter identifiera de områden där det finns en större risk att en incident kan uppstå. Utifrån analyserna kan myndigheterna sedan använda olika instrument för att upptäcka ett säkerhetshot. Dessa kan vara både tekniska och organisatoriska åtgärder. Utgångspunkten är att de vidtagna säkerhetsåtgärderna ska ge tillräckligt skydd och att incidenter inte ska inträffa.

Exempel på tekniska åtgärder är bl.a. intrångsdetektorer som automatiskt analyserar och upptäcker dataintrång och användning av logganalysinstrument för att kunna detektera obehörig åtkomst (loggavvikelser). En ökad insikt om verksamhetens ”normala” nätverks

trafikmönster hjälper till att identifiera sådant som avviker från den normala trafikbilden gentemot exempelvis servrar, applikationer eller datafiler. Organisatoriska åtgärder kan exempelvis vara antagande av interna strategier för dataskydd som avser interna regler, riktlinjer, rutiner och olika typer av styrdokument och policydokument.[10] Riktlinjer och regler för hantering av personuppgifter, rutiner för incidenthantering och logguppföljning[11] utgör exempel på sådana strategier. Periodisk uppföljning av tilldelade behörigheter är ett annat exempel på organisatoriska åtgärder. I en behörig myndighet ska det finnas rutiner för tilldelning, förändring, borttagning och regelbunden kontroll av behörigheter.[12] Information till och utbildning av personal om de regler och rutiner för incidenthantering som ska följas är också exempel på sådana åtgärder.

Datainspektionens bedömning
Polismyndigheten har i huvudsak uppgett följande. Myndighetens IT-miljö säkerhetsövervakas kontinuerligt, dygnet runt, i syfte att förebygga, upptäcka och förhindra exempelvis it-attacker, driftstörningar och spridning av skadlig kod. Därigenom kan allvarligare personuppgiftsincidenter upptäckas i ett tidigt skede. Om det finns anledning till närmare utredning av användaraktiviteter kan loggutdrag användas. Utöver detta har varje enskild medarbetare ett eget ansvar att rapportera alla händelser där risk finns att information har skadats, ändrats, förstörts, röjts eller någon kan ha givits obehörig åtkomst till information. Angående organisatoriska åtgärder framgår av utredningen att Polismyndigheten har rutiner för att rapportera personuppgiftsincidenter internt och att det på myndighetens intranät finns information om hur och när rapporteringen ska göras. Polismyndigheten har dessutom tagit fram en generell informationssäkerhetsutbildning, som under våren 2019 gjorts tillgänglig för samtliga medarbetare på myndigheten. I utbildningen ingår ett avsnitt om incidenter, vilket även inbegriper personuppgiftsincidenter. Myndigheten ställer numera ett krav på att samtliga medarbetare ska genomföra utbildningen för att få tillgång till myndighetens IT-system.

---

[10] Brottsdatalag – Delbetänkande av Utredningen om 2016 års dataskyddsdirektiv Stockholm 2017, SOU 2017:29 s. 302
[11] Behöriga myndigheter ska se till att det finns rutiner för logguppföljning, se prop. 2017/18:232 s. 455 f.
[12] 3 kap. 6 § BDL och kompletterande bestämmelser i 3 kap. 6 § BDF

Datainspektionen kan konstatera att Polismyndigheten har rutiner för att upptäcka personuppgiftsincidenter på plats.

Skyldigheten att vidta säkerhetsåtgärder för att upptäcka personuppgiftsincidenter är inte knuten till en viss tidpunkt utan åtgärderna ska kontinuerligt ses över och vid behov förändras. För att Polismyndigheten ska kunna upprätthålla tillräcklig skyddsnivå av personuppgifter över tid rekommenderar Datainspektionen, med stöd av 5 kap. 6 § BDL, att myndigheten regelbundet utvärderar effektiviteten hos de vidtagna säkerhetsåtgärderna för att upptäcka personuppgiftsincidenter och att myndigheten vid behov uppdaterar dessa.

Rutiner för hantering av personuppgiftsincidenter

För att kunna leva upp till kraven på organisatoriska åtgärder i 3 kap. 8 § BDL ska den personuppgiftsansvarige ha dokumenterade interna rutiner som beskriver vilken process som ska följas när en incident har upptäckts eller inträffat, inbegripet hur incidenten ska begränsas, hanteras och återställas, samt hur riskbedömningen ska gå till och hur incidenten ska anmälas internt och till Datainspektionen. Av rutinerna ska framgå bl.a. vad en personuppgiftsincident är/kan vara, när en incident behöver anmälas, och till vem, vad som ska dokumenteras, ansvarsfördelningen samt vilken information som bör tillhandahållas inom ramen för anmälan till Datainspektionen.

Datainspektionens kontroll av rutiner för att hantera personuppgiftsincidenter avser tiden från brottsdatalagens ikraftträdande dvs. den 1 augusti 2018.

Datainspektionens bedömning

Polismyndigheten har i huvudsak uppgett följande. Av information på Polismyndighetens intranät framgår hur en rapportering av en personuppgiftsincident ska hanteras. Personuppgiftsincidenter hanteras som andra typer av incidenter och rapporteras i myndighetens incidenthanteringssystem POINT. I ett kompletterande svar tydliggör Polismyndigheten att det stämmer att det inte fanns några nationella riktlinjer för hantering av personuppgiftsincidenter när BDL trädde i kraft men detta innebär inte att rutiner saknades. Rutinerna har tagits fram av rättsavdelningen och dataskyddsombudet i samråd med IT-avdelningen, de har dokumenterats inom rättsavdelningen och har därmed varit tillgängliga

för de personer som arbetar med att hantera och bedöma personuppgiftsincidenter. Information om vad som kan vara en personuppgiftsincident och vad en medarbetare ska göra om han eller hon misstänker att en sådan inträffat har bland annat funnits på polisens intranät och i grundläggande dataskyddsutbildningar.

Det framgår vidare att myndigheten inför brottsdatalagens införande gjorde en bedömning att befintliga strukturer och system för incidentrapportering kunde användas även för att upptäcka, anmäla och hantera personuppgiftsincidenter. Vid den tidpunkten ansåg Polismyndigheten att de rutindokument som fanns var tillräckliga även för att hantera personuppgiftsincidenter. Med anledning av detta utarbetades inledningsvis inga nya nationella riktlinjer utan det gjordes enbart en intern ansvarsfördelning samt enhetsspecifika rutiner för åtgärder vid hanteringen. Polismyndigheten har dock uppmärksammat ett ökat behov av att i riktlinjer formalisera de rutiner som tidigare arbetats fram. Detta för att tydliggöra ansvars- och rollfördelningen mellan olika organisatoriska enheter och skapa en större medvetenhet om vikten av att identifiera och anmäla personuppgiftsincidenter i hela myndigheten. Polismyndigheten uppger vidare att myndigheten kontinuerligt har utvärderat och uppdaterat sina skriftliga rutiner om hur personuppgiftsincidenter ska hanteras sedan de nya dataskyddsreglerna började tillämpas under sommaren 2018. Rutiner för att hantera personuppgiftsincidenter har alltså funnits sedan sommaren 2018. Senaste versionen *Rutin för personuppgiftsincident* daterad 2020-05-28 har myndigheten lämnat in. Polismyndigheten har även *lämnat in den information från myndighetens intranät* som har varit tillgänglig för alla medarbetare sedan juli 2018.

Med beaktande av de inlämnande handlingarna och vad som framkommit i ärendet konstaterar Datainspektionen att Polismyndigheten från tidpunkten då brottsdatalagen trädde ikraft har haft och har rutiner för att hantera personuppgiftsincidenter på plats.

Att kunna hantera upptäckta personuppgiftsincidenter på ett korrekt sätt och motverka dess effekter och risker för de registrerades personliga integritet är viktigt. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Polismyndigheten regelbundet kontrollerar att rutinerna för hantering av personuppgiftsincidenter följs.

Rutiner för dokumentation av personuppgiftsincidenter

En förutsättning för att Datainspektionen ska kunna kontrollera efterlevnaden av dokumentationskravet av incidenter i 3 kap. 14 § BDF är att dokumentationen omfattar vissa uppgifter som alltid bör ingå. Dokumentationen ska omfatta alla detaljer kring incidenten, inbegripet dess orsaker, vad som skedde och de personuppgifter som berördes. Den ska även innehålla incidentens konsekvenser och de korrigerande åtgärder som den personuppgiftsansvarige vidtagit.

Datainspektionens bedömning

Polismyndigheten har huvudsakligen uppgett följande. Myndigheten använder sig av incidenthanteringssystemet POINT för rapportering av bl.a. personuppgiftsincidenter. Rättsavdelningen dokumenterar de händelser som bedöms vara en personuppgiftsincident i särskild ordning. Av rättsavdelningens dokumentation framgår information om bl.a. datum då incidenten upptäcktes, datum då incidenten bedömdes vara en personuppgiftsincident, en kort beskrivning av personuppgiftsincidenten, aktuell lagstiftning (dataskyddsförordningen eller brottsdatalagen). Vidare framgår även om incidenten har anmälts till Datainspektionen, ärendenummer i POINT och eventuellt ärendenummer i Polisens allmänna diarium (PÄR) som används om ärendet anmälts till Datainspektionen samt en rättslig bedömning med eventuellt underlag och eventuella synpunkter från dataskyddsombudet.

Datainspektionen konstaterar att Polismyndigheten har ett internt IT-system för att bl.a. rapportera personuppgiftsincidenter. Därutöver framgår av rättsavdelningens dokumentation till viss del vilka uppgifter som ska dokumenteras. Datainspektionen konstaterar dock att det av beskrivningen inte framgår vilka effekter som följer med en incident och vilka korrigerande åtgärder som vidtagits med anledning av den.

Att kunna dokumentera inträffade personuppgiftsincidenter på ett korrekt sätt och därmed motverka risken av att dokumentationen blir bristfällig eller ofullständig är viktigt. Bristfällig dokumentation kan leda till att incidenterna inte hanteras och åtgärdas på ett korrekt sätt, vilket kan få påverkan på integritetsskyddet. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Polismyndighetens rutiner för dokumentation av personuppgiftsincidenter kompletteras med de uppgifter som angetts i stycket ovan. Därutöver bör Polismyndigheten genomföra

regelbundna kontroller av den interna dokumentationen av personuppgiftsincidenter.

Information och utbildning kring personuppgiftsincidenter

Personalen är en viktig resurs i säkerhetsarbetet. Det räcker inte bara med interna rutiner, regler eller styrdokument om användarna inte följer dem. Alla användare måste förstå att hantering av personuppgifter ska ske på ett rättssäkert sätt samt att det är allvarligare att inte rapportera en incident än att rapportera t.ex. ett misstag eller ett fel. Det krävs därför att alla användare får en adekvat utbildning och tydlig information om dataskydd.

Den personuppgiftsansvarige ska informera och utbilda sin personal i frågor om dataskydd inbegripet hantering av personuppgiftsincidenter. Av Datainspektionens rapportserie *Anmälda Personuppgiftsincidenter* under perioden 2018-2019 framgår att den mänskliga faktorn utgör den vanligaste orsaken till anmälda personuppgiftsincidenter. [13] Dessa består i huvudsak av individer som, medvetet eller omedvetet, inte följer interna rutiner vid behandling av personuppgifter eller begått ett misstag vid hantering av personuppgifter. Omkring hälften av de incidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmeddelanden. Detta understryker enligt Datainspektionens mening betydelsen av att interna rutiner och tekniska säkerhetsåtgärder behöver kompletteras med löpande utbildning, information och andra åtgärder för att öka kunskap och medvetenhet hos medarbetarna.

Datainspektionens bedömning

På frågan om på vilket sätt information och utbildning om incidenter ges till anställda har Polismyndigheten uppgett bl.a. följande. På myndighetens intranät finns information om rapportering av personuppgiftsincidenter. Alla nyanställda på IT-avdelningen genomgår under sin introduktion en utbildning kring informationssäkerhetsincident och incidenthantering. Myndigheten har dessutom tagit fram en generell utbildning i informationssäkerhet som under våren 2019 gjorts tillgänglig för samtliga medarbetare. Polismyndigheten ställer numera krav på att alla medarbetare

[13] Rapport 2019:1, rapport 2019:3 och rapport 2020:2. Liknande slutsatser har MSB dragit i sin årsrapport för allvarliga IT-incidenter, dvs. att de flesta av incidenterna beror på mänskliga misstag, se https://www.msb.se/sv/aktuellt/nyheter/2020/april/arsrapporten-for-allvarliga-it-incidenter-2019-ar-slappt/

ska genomföra utbildningen för att få tillgång till myndighetens IT-system. I utbildningen ingår ett avsnitt om incidenter, vilket även inbegriper personuppgiftsincidenter. Avsnittet innehåller bland annat exempel på vilka incidenter som ska anmälas i POINT. Utöver denna utbildning finns ett flertal dataskyddsutbildningar i myndighetens läroplattform där bl.a. personuppgiftsincidenter beskrivs samt vikten att anmäla dessa påtalas.

Polismyndigheten har lämnat in myndighetens manual avseende ”Grundläggande dataskyddsutbildning” och ”Utbildning i EU:s dataskyddsförordning”. Av manualerna framgår ett avsnitt om hantering av personuppgiftsincidenter. Den grundläggande dataskyddsutbildningen riktar sig till samtliga anställda inom Polismyndigheten med tillgång till polisens datorsystem. Utbildningen riktar sig också till konsulter och andra uppdragstagare som behandlar information automatiserat inom ramen för sitt uppdrag. Utbildningen i EU:s dataskyddsförordning riktar sig främst till de som i sitt arbete på olika sätt behandlar personuppgifter inom polisens icke brottsbekämpande verksamhet. En motsvarande utbildning finns för personuppgiftsbehandling inom brottsdatalagens område.

Mot bakgrund av vad som framgår av utredningen anser Datainspektionen att Polismyndigheten har visat att myndigheten har gett information och utbildning om hantering av personuppgiftsincidenter till sina medarbetare.

För att upprätthålla kompetensen och säkerställa att ny personal får utbildning är det viktigt med återkommande information och utbildning till de anställda och inhyrd personal. Datainspektionen rekommenderar, med stöd av 5 kap. 6 § BDL, att Polismyndigheten ger de anställda löpande information och återkommande utbildningar i hanteringen av personuppgiftsincidenter och skyldigheten att rapportera dessa.

Detta beslut har fattats av enhetschefen Charlotte Waller Dahlberg efter föredragning av juristen Maria Angelica Westerberg. Vid den slutliga handläggningen av ärendet har även IT-säkerhetsspecialisten Ulrika Sundling och juristen Jonas Agnvall medverkat.

Charlotte Waller Dahlberg, 2020-12-17 (Det här är en elektronisk signatur)

Kopia för kännedom till:
Polismyndighetens dataskyddsombud

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Datainspektionen om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.